UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF TENNESSEE
NORTHEASTERN DIVISION

KIMBERLY GARNSEY, Individually, and on Behalf of All Others Similarly Situated,	)	
Plaintiff,	)	Case No.
v.	)	**JURY TRIAL DEMANDED**
CASH EXPRESS, LLC,	)	
Defendant.	)	

CLASS ACTION COMPLAINT

Plaintiff Kimberly Garnsey ("Plaintiff"), through her undersigned counsel, brings this action against Cash Express, LLC. ("Cash Express" or "Defendant") pursuant to the investigation of her attorneys, personal knowledge as to herself and her own acts and otherwise upon information and belief, and alleges as follows:

INTRODUCTION

1. Cash Express is a payday loan lender, check cashing service, and pawn shop with locations in Tennessee, Mississippi, Alabama, and Kentucky.

2. On or about September 15, 2022, Cash Express announced that it had been the recipient of a hack and exfiltration of sensitive personal information ("SPI") involving approximately 106,000 individuals who have used Defendant's services in the past (the "Data Breach").

3. Cash Express stated that the hack and exfiltration occurred between January 29 and February 6, 2022. Cash Express states that "[o]nce we identified the data that may have been affected, we promptly engaged a data review firm to determine what information was in those

files."[1] Cash Express further states that it did not receive those results until August 4, 2022. It then waited until September 15, 2022 to announce the occurrence of the hack.

4. Cash Express reported that this SPI included Social Security numbers, full names, dates of birth, contact information, driver's license numbers, "limited medical details," and financial information, including bank and routing numbers.

5. Plaintiff and Class members now face a present and imminent lifetime risk of identity theft, which is heightened here by the loss of Social Security numbers.

6. The information stolen in cyber-attacks allows the modern thief to assume victims' identities when carrying out criminal acts such as:

- Filing fraudulent tax returns;
- Using your credit history;
- Making financial transactions on behalf of victims, including opening credit accounts in victims' names;
- Impersonating victims via mail and/or email;
- Impersonating victims in cyber forums and social networks;
- Stealing benefits that belong to victims; and
- Committing illegal acts which, in turn, incriminate victims.

7. Plaintiff's and Class members' SPI was compromised due to Defendant's negligent and/or careless acts and omissions and its failure to protect the SPI of Plaintiff and Class members.

8. As of this writing, there exist many class members who have no idea their SPI has been compromised, and that they are at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

9. Plaintiff brings this action on behalf of all persons whose SPI was compromised as

[1] https://www.cashexpressllc.com/security-notice, last accessed October 4, 2022.

a result of Defendant's failure to: (i) adequately protect consumers' SPI, (ii) adequately warn its current and former customers and potential customers of its inadequate information security practices, and (iii) effectively monitor its platforms for security vulnerabilities and incidents (the "Class"). Defendant's conduct amounts to negligence and violates state statutes.

10. Plaintiff and similarly situated individuals have suffered injury as a result of Defendant's conduct. These injuries include: (i) lost or diminished inherent value of SPI; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their SPI; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iv) deprivation of rights they possess under Tennessee data privacy laws; and (v) the continued and certainly an increased risk to their SPI, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the SPI.

JURISDICTION AND VENUE

11. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant.

12. This Court has personal jurisdiction over Defendant because Defendant's principal places of business is located within this District.

13. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to these claims occurred in, were directed to, and/or emanated from this District. Defendant resides within this judicial district and a substantial part of the events giving rise to the claims alleged herein occurred within this judicial district.

PARTIES

14. Plaintiff Kimberly Garnsey is a natural person residing in Drummonds, Tennessee. On or about September 19, 2022, Plaintiff Garnsey was informed via letter dated August 26, 2022 that she had been a victim of the Data Breach.

15. Defendant Cash Express, LLC is a Tennessee limited liability corporation with its principal place of business at 345 S. Jefferson Ave., Suite 403, Cookeville, Tennessee 38501.

FACTUAL ALLEGATIONS

16. Defendant is a loan company, dealing in payday loans, installment loans, small lines of credit, pawn loans, gold purchases, title loans, and check cashing services.[2]

17. In the normal course of business, Cash Express collects SPI from individuals who take out various loans with Cash Express. This SPI includes Social Security Numbers, driver's license numbers, bank account numbers, routing numbers, and apparently some medical information. Cash Express also collects customers' full names, dates of birth, addresses, phone numbers, and other contact information.

18. Cash Express's Privacy Policy states, "[t]o protect our personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings."[3] Cash Express further states that it does not share information with entities that are not affiliates.[4]

19. On or about September 15, 2022, Defendant announced:

> On February 6, 2022, Cash Express became aware of unusual activity on our network. We promptly began working with cybersecurity experts to investigate

---

[2] *See* https://www.cashexpressllc.com/, last accessed October 4, 2022
[3] https://www.cashexpressllc.com/uploads//Cash_Express_Privacy_Policy_July_2021.pdf, last accessed October 4, 2022.
[4] *Id.*

> and subsequently determined that an unauthorized third-party gained access to a portion of our computer system. Based on our investigation, we believe they had access from January 29, 2022, to February 6, 2022. Once we identified the data that may have been affected, we promptly engaged a data review firm to determine what information was in those files. We received those results on August 4, 2022. And we are now providing you this notice to give you information on what happened and what we are doing in response.[5]

20. Cash Express conceded that the hacker gained access, including SPI in the form of "full name, date of birth, contact information, government identification (such as Social Security or driver's license number), limited medical details, and financial information (such as bank account and routing number)."[6]

21. As of this writing, Defendant has offered minimal concrete information on the steps it has taken or specific efforts made to reasonably ensure that such a breach cannot or will not occur again.

22. Defendant is offering a wholly inadequate solitary year of credit monitoring from Experian Identity works to all affected customers, including Plaintiff and the Class.

23. This response is entirely inadequate to Plaintiff and Class members who now face several years of heightened risk from the theft of their SPI and who may have already incurred substantial out-of-pocket costs in responding to the Data Breach.

24. This is particularly problematic because Plaintiff's and Class members' SPI was in the hands of hackers for approximately seven and a half months before Defendant began notifying them of the Data Breach.

25. Defendant had obligations created by contract, industry standards, common law, and representations made to Plaintiff and Class members, to keep their SPI confidential and to

---

[5] https://www.cashexpressllc.com/security-notice, last accessed October 4, 2022.
[6] *Id.*

protect it from unauthorized access and disclosure.

26. Furthermore, this is not Cash Express's first data breach. In 2015, a Cash Express employee was charged with using the information of former customers to fraudulently open loans.[7]

27. Plaintiff and Class members provided their SPI to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

28. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches preceding the date of the breach.

29. Indeed, data breaches, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known and completely foreseeable to the public and to anyone in Defendant's industry, including Defendant.

30. According to the Federal Trade Commission ("FTC"), identity theft wreaks havoc on consumers' finances, credit history, and reputation and can take time, money, and patience to resolve.[8] Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank and finance fraud.[9]

---

[7] *See* https://www.databreaches.net/ky-former-cash-express-employee-arrested/, last accessed October 4, 2022.

[8] *See Taking Charge, What to Do If Your Identity is Stolen*, FTC, 3 (Apr. 2013), https://dss.mo.gov/cd/older-youth-program/files/taking-charge-what-to-do-if-identity-is-stolen.pdf, last accessed October 4, 2022.

[9] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 CFR § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." *Id*.

31. The SPI of Plaintiff and Class members was taken by hackers to engage in identity theft and/or to sell to other criminals who purchase SPI for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years, requiring Plaintiff and Class members to remain vigilant well into the future.

32. Defendant knew, or reasonably should have known, of the importance of safeguarding the SPI of Plaintiff and Class members, including Social Security numbers, dates of birth, and other sensitive information, as well as of the foreseeable consequences that would occur if Defendant's data security systems were breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class members as a result of a breach.

33. Plaintiff and Class members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their SPI.

34. Plaintiff's and Class members' injuries were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the SPI of Plaintiff and Class members.

35. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

36. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their networks' vulnerabilities; and implement policies to correct any

security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

37. The FTC further recommends that companies not maintain SPI longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

38. The FTC has brought enforcement actions against businesses for failing to protect consumer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

39. Defendant failed to properly implement basic data security practices, and its failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer SPI constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

40. A number of industry and national best practices have been published and should have been used as a go-to resource and authoritative guide when developing Defendant's cybersecurity practices.

41. Best cybersecurity practices include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers;

monitoring and protecting physical security systems; protecting against any possible communication system; and training staff regarding critical points.

42. Upon information and belief, Defendant failed to meet the minimum standards of the following cybersecurity frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established standards in reasonable cybersecurity readiness.

43. These foregoing frameworks are existing and applicable industry standards in Defendant's industry, but Defendant failed to comply with these accepted standards, thereby opening the door to the cyber-attack and causing the Data Breach.

44. Businesses that store personal information are likely to be targeted by cyber criminals, and this is particularly true in regard to credit card and bank account numbers. However, information such as dates of birth and Social Security numbers are even more attractive to hackers because they are not easily destroyed and can be easily used to perpetrate identity theft and other types of fraud.

45. Individuals' SPI is highly valuable to criminals, as evidenced by the prices they will pay to purchase this information via the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold for $40 to $200, and bank details have a price range of $50 to $200.[10]

46. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration ("SSA") stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive

[10] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs, last accessed October 4, 2022

financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[11]

47. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

48. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[12]

49. Furthermore, as the SSA warns:

> Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you should not be able to use the old number anymore.

---

[11] SSA, *Identity Theft and Your Social Security Number*, SSA Publication No. 05-10064 (Jun. 2018), https://www.ssa.gov/pubs/EN-05-10064.pdf, last accessed October 4, 2022.

[12] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015),http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft, last accessed October 4, 2022.

> For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under the new number may make more difficult for you to get credit.[13]

50. Here, the unauthorized access left the cyber criminals with the tools to perform the most thorough identity theft—they have obtained all the essential SPI to mimic the identity of the user. Plaintiff's and Class members' stolen personal data is a dream for hackers and a nightmare for Plaintiff and the Class. The personal data stolen in conjunction with the Data Breach essentially provides one-stop shopping for identity thieves.

51. A person whose personal information has been compromised may not see any signs of identity theft for years, and public policy supports an approach wherein businesses act vigilantly to monitor, detect, guard against, and prevent fraudulent activity. According to the United States Government Accountability Office ("GAO") Report to Congressional Requesters:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[14]

52. Companies recognize that SPI is a valuable asset–indeed, it is a valuable commodity. A "cyber black-market" exists in which criminals openly post stolen Social Security numbers and other SPI on a number of Internet websites. The stolen personal data of Plaintiff and Class members is highly valuable on both legitimate and black markets.

53. Identity thieves may commit various types of crimes such as immigration fraud, obtaining a driver license or identification card in the victim's name but with another person's picture, and/or using the victim's information to obtain a fraudulent tax refund or fraudulent

---

[13] SSA, *Identity Theft and Your Social Security Number*, SSA Publication No. 05-10064 (Jun. 2018), http://www.ssa.gov/pubs/EN-05-10064.pdf, last accessed October 4, 2022.

[14] *See* https://www.gao.gov/assets/gao-07-737.pdf (June 2007) at 29, last accessed October 4, 2022.

unemployment benefits. The United States government and privacy experts acknowledge that it may take years for identity theft to come to light and be detected.

54. As noted above, the disclosure of Social Security numbers in particular poses a significant risk. Criminals can, for example, use Social Security numbers to create false bank accounts or file fraudulent tax returns. Defendant's former and current customers whose Social Security numbers have been compromised now face a real, present, imminent and substantial risk of identity theft and other problems associated with the disclosure of their Social Security number and will need to monitor their credit and tax filings for an indefinite duration.

55. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because credit and debit card accounts can easily and quickly be closed. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change — Social Security number, driver license number or government-issued identification number, name, and date of birth.

56. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[15]

57. This is even more true for minors, whose Social Security Numbers are particularly valuable. As one site noted, "The organization added that there is extreme credit value in Social Security numbers that have never been used for financial purposes. It's relatively simple to add a false name, age or address to a Social Security number. After that happens, there is a window for

[15] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html, last accessed October 4, 2022

thieves to open illicit credit cards or even sign up for government benefits."[16]

58. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, housing, or even give false information to police. An individual may not know that his or her driver's license was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud, or until the individual attempts to lawfully apply for unemployment and is denied benefits (due to the prior, fraudulent application and award of benefits).

FACTS SPECIFIC TO PLAINTIFF

59. On or about September 19, 2022, Plaintiff was notified via a physical letter (dated September 15, 2022) from Defendant that she had been the victim of the Data Breach.

60. Plaintiff has experienced a surge in spam calls and texts roughly coincident with the timing of the Data Breach, indicating that hackers are already trying to take advantage of the release of her SPI.

61. Additionally, Plaintiff is aware of no other source from which the theft of her SPI could have come. She regularly takes steps to safeguard her own SPI in her own control.

CLASS ACTION ALLEGATIONS

62. Plaintiff brings this nationwide class action pursuant to Rules 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure, individually and on behalf of all members of the following classes:

> Nationwide Class: All natural persons residing in the United States whose SPI was compromised in the Data Breach announced by Defendant on or about September 12, 2022 (the "Nationwide Class").
>
> Tennessee Subclass: All natural persons residing in Tennessee whose SPI was

[16] https://www.identityguard.com/news/kids-targeted-identity-theft, last accessed September 6, 2022)

compromised in the Data Breach announced by Defendant on or about September 12, 2022 (the "Tennessee Subclass").

63. Excluded from the Classes are all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out, and all judges assigned to hear any aspect of this litigation and their immediate family members.

64. Plaintiff reserves the right to modify or amend the definitions of the proposed Classes before the Court determines whether certification is appropriate.

65. **Numerosity**: The Classes are so numerous that joinder of all members is impracticable. One security website has, as of this writing, indicated that the total number of Class Members is approximately 106,521.[17] The identity of individual members of the Classes is readily identifiable from records in Defendant's possession and/or control.

66. **Commonality**: Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual members of the Classes. These include:

a. When Defendant actually learned of the Data Breach and whether its response was adequate;

b. Whether Defendant owed a duty to the Classes to exercise due care in collecting, storing, safeguarding and/or obtaining their SPI;

c. Whether Defendant breached that duty;

d. Whether Defendant implemented and maintained reasonable security procedures and practices appropriate to the nature of storing the SPI of Plaintiff and members of the Classes;

e. Whether Defendant acted negligently in connection with the monitoring and/or protection of SPI belonging to Plaintiff and members of the Classes;

f. Whether Defendant knew or should have known that it did not employ reasonable measures to keep the SPI of Plaintiff and members of the Classes secure and to prevent loss or misuse of that SPI;

---

[17] *See* https://apps.web.maine.gov/online/aeviewer/ME/40/8f4fd997-6635-481c-ba23-4e3cc7015938.shtml, last accessed October 4, 2022

g. Whether Defendant has adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

h. Whether Defendant caused Plaintiff's and members of the Classes damage;

i. Whether Defendant violated the law by failing to promptly notify Plaintiff and members of the Classes that their SPI was compromised; and

j. Whether Plaintiff and the other members of the Classes are entitled to credit monitoring and other monetary relief.

67. **Typicality**: Plaintiff's claims are typical of those of the other members of the Classes because all had their SPI compromised as a result of the Data Breach due to Defendant's misfeasance.

68. **Adequacy**: Plaintiff will fairly and adequately represent and protect the interests of the Classes. Plaintiff's counsel is competent and experienced in litigating privacy-related class actions.

69. **Superiority and Manageability**: Under rule 23(b)(3) of the Federal Rules of Civil Procedure, a class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all the members of the Classes is impracticable. Individual damages for any individual member of the Classes are likely to be insufficient to justify the cost of individual litigation, so that in the absence of class treatment, Defendant's misconduct would go unpunished. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action.

70. Class certification is also appropriate under Rule 23(a) and (b)(2) because Defendant has acted or refused to act on grounds generally applicable to the Classes, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Nationwide Class as a whole and as to the Tennessee Subclass as a whole.

71. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would

advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiff and members of the Classes to exercise due care in collecting, storing, using, and safeguarding their SPI;

b. Whether Defendant breached a legal duty to Plaintiff and the members of the Classes to exercise due care in collecting, storing, using, and safeguarding their SPI;

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach; and

e. Whether members of the Classes are entitled to actual damages, credit monitoring or other injunctive relief, and/or punitive damages as a result of Defendant's wrongful conduct.

FIRST CLAIM FOR RELIEF
Breach of Implied Contract
(By Plaintiff Individually and on Behalf of the Nationwide Class)

72. Plaintiff hereby re-alleges and incorporates by reference all of the allegations in paragraphs 1 to 71.

73. When Plaintiff and Class Members provided their SPI to Defendant in exchange for Defendant's services, they entered into implied contracts with Defendant under which—and by mutual assent of the parties—Defendant agreed to take reasonable steps to protect their SPI.

74. Defendant solicited and invited Plaintiff and Class Members to provide their SPI as part of Defendant's regular business practices and as essential to the services transactions entered into between Defendant on the one hand and Plaintiff and Class Members on the other. This conduct thus created implied contracts between Plaintiff and Class Members on the one hand, and Defendant on the other hand. Plaintiff and Class Members accepted Defendant's offers by

providing their SPI to Defendant in connection with their purchases from Defendant.

75. When entering into these implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws, regulations, and industry standards.

76. Defendant's implied promise to safeguard Plaintiff's and Class Members' SPI is evidenced by a duty to protect and safeguard SPI that Defendant required Plaintiff and Class Members to provide as a condition of entering into consumer transactions with Defendant.

77. Plaintiff and Class Members paid money to Defendant to purchase services from Defendant. Plaintiff and Class Members reasonably believed and expected that Defendant would use part of funds received as a result of the transactions to obtain adequate data security. Defendant failed to do so.

78. Plaintiff and Class Members, on the one hand, and Defendant, on the other hand, mutually intended—as inferred from use of Defendant's services—that Defendant would adequately safeguard SPI. Defendant failed to honor the parties' understanding of these contracts, causing injury to Plaintiff and Class Members.

79. Plaintiff and Class Members value data security and would not have provided their SPI to Defendant in the absence of Defendant's implied promise to keep the SPI reasonably secure.

80. Plaintiff and Class Members fully performed their obligations under their implied contracts with Defendant.

81. Defendant breached its implied contracts with Plaintiff and Class Members by failing to implement reasonable data security measures and permitting the Data Breach to occur.

82. As a direct and proximate result of Defendant's breaches of the implied contracts, Plaintiff and Class Members sustained damages as alleged herein and are thereby entitled to compensatory, consequential, and other damages suffered as a result of the Data Breach.

83. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide credit monitoring and identity theft insurance to Plaintiff and Nationwide Class members.

SECOND CLAIM FOR RELIEF
Unjust Enrichment, in the Alternative
(By Plaintiff Individually and on Behalf of the Nationwide Class)

84. Plaintiff hereby re-alleges and incorporates by reference all of the allegations in paragraphs 1 to 71.

85. Plaintiff and Class Members conferred a monetary benefit upon Defendant in the form of storing their SPI with Defendant in such a way that saved expense and labor for Defendant.

86. Defendant appreciated or had knowledge of the benefits conferred upon it by Plaintiff and Class Members. Defendant also benefited from the receipt of Plaintiff's and Class Members' SPI, as this was used by Defendant to facilitate its core functions.

87. The benefits given by Plaintiff and Class Members to Defendant were to be used by Defendant, in part, to pay for or recoup the administrative costs of reasonable data privacy and security practices and procedures.

88. As a result of Defendant's conduct, Plaintiff and Class Members suffered actual damages in an amount to be determined at trial.

89. Under principles of equity and good conscience, Defendant should not be permitted to retain a benefit belonging to Plaintiff and Class Members because Defendant failed to

implement (or adequately implement) the data privacy and security practices and procedures that Plaintiff and Class Members granted to Defendant or were otherwise mandated by federal, state, and local laws and industry standards.

90. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds or benefits it received as a result of the conduct alleged herein.

THIRD CLAIM FOR RELIEF
Violations of the Tennessee Identity Theft Deterrence Act of 1999
Tenn. Code Ann § 47-18-2101, *et seq.*
(By Plaintiff Individually and on behalf of the Tennessee Subclass)

91. Plaintiff hereby re-alleges and incorporates by reference all the allegations in paragraphs 1 to 71.

92. Defendant is a business that owns or licenses computerized data that includes Personal Information as defined by Tenn. Code Ann. § 47-18-2107(a)(2).

93. Plaintiff and Tennessee Subclass members' Personal Information that was compromised in the Data Breach includes Personal Information as covered under Tenn. Code Ann. § 47-18-2107(a)(3)(A).

94. Defendant is required to accurately notify Plaintiff and Tennessee Subclass members if it becomes aware of a breach of its data security systems that is reasonably likely to have caused unauthorized persons to acquire Plaintiff's and Tennessee Subclass members' Personal Information in the most expedient time possible and without unreasonable delay under Tenn. Code Ann. § 47-18-2107(b).

95. Because Defendant discovered a breach of its security systems in which unencrypted PII and PHI was, or is reasonably believed to have been, acquired by an unauthorized

person, Defendant has an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Tenn. Code Ann. § 47-18-2107(b).

96. By failing to disclose the Data Breach in a timely and accurate manner, Defendant violated Tenn. Code Ann. § 47-18-2107(b).

97. As a direct and proximate result of Defendant's violations of Tenn. Code Ann. § 47-18-2107(b), Plaintiff and Tennessee Subclass members suffered damages, as described above.

98. Plaintiff and Tennessee Subclass members seek relief under Tenn. Code Ann. §§ 47-18-2107(h), 47-18-2104(d), and 47-18-2104(f), including actual damages and injunctive relief.

FOURTH CLAIM FOR RELIEF
Violations of the Tennessee Consumer Protection Act of 1977,
Tenn. Code. Ann § 47-18-101, *et seq.*
(By Plaintiff Individually and on Behalf of the Tennessee Subclass)

99. Plaintiff hereby re-alleges and incorporates by reference all the allegations in paragraphs 1 to 71.

100. Tenn. Code Ann. § 47-18-109(a)(1) provides that "[a]ny person who suffers an ascertainable loss of money or property, real, personal, or mixed, or any other article, commodity, or thing of value wherever situated, as a result of the use or employment by another person of an unfair or deceptive act or practice described in § 47-18-104(b) and declared to be unlawful by this part, may bring an action individually to recover actual damage."

101. Tenn. Code Ann. § 47-18-109(a)(3) further provides that "[i]f the court finds that the use or employment of the unfair or deceptive act or practice was willful or knowing violation of this part, the court may award three (3) times the actual damages sustained and may provide such other relief as it considers necessary and proper…."

102. Defendant's lending, check cashing, sales, and other services constitute "trade or commerce."

103. Defendant's conduct violates the Tennessee Consumer Protection Act because Defendant engaged in the deceptive acts and practices described above, which included a failure to protect Plaintiff's and the Tennessee Subclass's Personal Information in spite of assurances to the contrary.

104. Defendant omitted material facts concerning the steps they took (or failed to undertake) to protect Plaintiff and Tennessee Subclass members' Personal Information, which is deceptive, false, and misleading given the conduct described herein. Such conduct is inherently and materially deceptive and misleading in a material respect, which Defendant knew, or by the exercise of reasonable care, should have known, to be untrue, deceptive or misleading. Such conduct is unfair, deceptive, untrue, or misleading in that Defendant: (a) represented that their services have approval, characteristics, uses or benefits that they do not have; and (b) represented that services are of a particular standard, quality or grade.

105. Defendant's materially misleading statements and deceptive acts and practices alleged herein were directed at the public at large.

106. Defendant's actions impact the public interest because Plaintiff and the Tennessee Subclass have been injured in exactly the same way as thousands of others as a result of and pursuant to Defendant's generalized course of deception as described throughout this Complaint.

107. Defendant's acts and practices described above were likely to mislead a reasonable consumer acting reasonably under the circumstances.

108. Defendant's misrepresentations, misleading statements and omissions were materially misleading to Plaintiff and members of the Tennessee Subclass.

109. Defendant's violation of Tenn. Code Ann. § 47-18-104 was willful and knowing. As described above, at all relevant times, Defendants, among other things, knew that their policies

and procedures for the protection of Plaintiff's and the Tennessee Subclass's PII and PHI were inadequate to protect that PII and PHI. Nonetheless, Defendant continued to solicit and process PII and PHI in the United States in order to increase their own profits.

110. Had Plaintiff and the members of the Tennessee Subclass known of Defendant's misrepresentations, misleading statements and omissions about their use of PII and PHI, they would not have used Defendant's services or given Defendant their PII and PHI.

111. As a direct and proximate result of Defendant's conduct in violation of Tenn. Code Ann. § 47-18-104, Plaintiff and the members of the Tennessee Subclass have been injured in amounts to be proven at trial.

112. As a result, pursuant to Tenn. Code Ann. §§ 47-18-104 and 47-18-109, Plaintiff and the Tennessee Subclass are entitled to damages in an amount to be determined at trial. Plaintiff also properly asks that such damages be trebled based on Defendant's knowledge and/or intention with respect to its breach.

113. Plaintiff also seeks injunctive relief, including the dissemination of a factually accurate statement on the actual state of Defendant's PII and PHI storage and security posture.

114. Additionally, pursuant to Tenn. Code Ann. § 47-18-109, Plaintiff and the Tennessee Subclass make claims for attorneys' fees and costs.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and all Class Members, requests judgment against the Defendant and the following:

A. For an Order certifying the Class as defined herein and appointing Plaintiff and her counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct

complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and the Class Members' SPI;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the personal identifying information of Plaintiff and Class Members' personal identifying information;

iv. prohibiting Defendant from maintaining Plaintiff's and Class Members' personal identifying information on a cloud-based database (if, in fact, it does so);

v. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vi. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

vii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

viii. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

ix. requiring Defendant to conduct regular database scanning and security checks;

x. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xi. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing

employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiii. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xiv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xv. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and

xvi. for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment; and

D. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For pre- and post-judgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

JURY DEMAND

Plaintiff hereby demands a trial by jury on all issues so triable.

DATED: October 7, 2022

Respectfully Submitted,

By: /s/ *R. Luke Widener*

R. Luke Widener
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
800 S. Gay St., Ste. 1100
Knoxville, TN 37929
Telephone: (865)-247-0080
lwidener@milberg.com
As Local Counsel

Carl V. Malmstrom
WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLC
111 W. Jackson Blvd., Suite 1700
Chicago, Illinois 60604
Tel: (312) 984-0000
Fax: (212) 686-0114
malmstrom@whafh.com

Attorney for Plaintiff and the Putative Class